آشنایی با ویروس های کامپیوتری

پیش از شروع بد نیست تا این نکته را هم بدانید که در حالت دسته بندی کلی تر می توان همه ویروسها را به دو نوع زیر تقسیم بندی نمود:

- **ویروسهای با عملکرد مستقیم (Direct Action Viruses)**
- **ویروسهای با عملکرد غیر مستقیم یا ویروسهای مقیم در حافظه** (Non Direct Action or Memory Resident Viruses)

لازم به ذکر است که ویروس ها می توانند همزمان خصوصیات هر دو دسته را نیز داشته باشند. ویروسهای مقیم در حافظه می توانند همه اعمال سیستم را زیر نظر بگیرند و به محض اجرا شدن یک برنامه یا سایر دسترسی ها، برنامه های دیگر را آلوده نمایند.

ویروسها به دو روش کلی در حافظه مقیم می شوند:

- **با استفاده از وقفه ها**

- **با استفاده از دستکاری زنجیره (Memory Control Block یا MCB) در حافظه**

البته سیستم عامل ویندوز حالت در حافظه مقیم بودن ویروسها را که از جهاتی یک امتیاز محسوب می شود، تقریبا از بین برده است، به همین دلیل امروزه شاهد ظهور بسیاری از ویروسهایی هستیم که علاوه بر مقیم بودن در حافظه، توانائی عملکرد مستقیم را نیز دارند!

ویروسهای باینری فایل:

یک ویروس فایلی خودش را به یک فایل برنامه (یا در اصطلاح میزبان) ضمیمه می نماید و از تکنیکهای مختلفی برای آلوده ساختن فایل های اجرایی دیگر استفاده می کند. ویروسهای فایلی بر اساس بکار بردن این تکنیکها به انواع مختلف تقسیم می شوند، مهمترین این انواع به شرح زیر می باشند:

- **ویروسهای رونویسی کننده (Overwriting Viruses):**

ویروسهای رونویسی کننده خودشان را در ابتدای برنامه و مستقیما روی کدهای آن جایگزین می نمایند، بنابراین برنامه اصلی آسیب دیده و تبدیل به یک ویروس می شود، پس وقتی تلاش می کنیم تا این برنامه را اجرا نماییم نه تنها برنامه اجرا نمی شود بلکه ویروس فایلهای دیگری را نیز آلوده می نماید. این ویروسها را می توان به راحتی شناسایی و نابود کرد برای همین میزان پراکندگی آنها بسیار ناچیز است.

- **ویروسهای همراه (Companion Viruses):**

ویروسهای همراه میزبانشان را مستقیما تغییر نمی دهند و بجای این کار با ترفندهایی باعث می شوند تا سیستم عامل ویروس را به جای برنامه مورد نظر اجرا نماید. گاهی این کار با تغییر دادن نام فایل میزبان به نامی دیگر و واگذاری نام آن برنامه به ویروس، انجام می شود.

در برخی مواقع هم ویروس، فایل EXE را از طریق تولید یک فایل COM به همان نام و در همان دایرکتوری، آلوده می نماید. به این

ترتیب که سیستم عامل داس همیشه یک فایل COM هم نام با یک فایل EXE را ابتدا اجرا می نماید.

- ویروسهای پیوند دهنده (Link Viruses):

ویروسهای پیوند دهنده تغییراتی را در طرز کار سطح پائین (Low Level) سیستم فایل می دهند این تغییرات موجب می شود که نام برنامه تا مدتها بجای پیوند (اشاره داشتن) به فایل برنامه به کپی ویروس پیوند داده شود. این امکان نیز فراهم است تا نام همه برنامه ها به فایل ویروس اشاره داشته باشند.

- ویروسهای ابتدا قرار گیرنده (Prepending Viruses):

این ویروسها به سادگی کدشان را در بالای برنامه اصلی قرار می دهند، بنابراین در زمان اجرای برنامه ای که توسط ویروسهای ابتدا قرار گیرنده آلوده شده باشد، کد ویروس قبل از برنامه اصلی اجرا می گردد.

- **ویروسهای داخل شونده (Inserting Viruses):**

ویروسهای داخل شونده خودشان را در میان برنامه میزبان کپی می نمایند. گاهی اوقات برنامه ها دارای فضاهای استفاده نشده ای هستند، این ویروسها می توانند چنین فضاهایی را یافته و خودشان را در میان آنها وارد نمایند.

این ویروسها همچنین می توانند طوری طراحی شوند که قطعه بزرگی از برنامه میزبان را به جای دیگری منتقل نموده و به سادگی از فضای خالی استفاده نمایند.

- **ویروسهای اضافه شونده (Appending Viruses):**

این ویروسها پرشی را در ابتدای فایل برنامه قرار می دهند، قسمت ابتدائی فایل برنامه اصلی را به انتهای آن جابجا می نمایند و خودشان را در بین قسمت انتهائی فایل برنامه اصلی و قسمت ابتدائی آن جایگزین می نمایند. بنابراین در زمان اجرای چنین برنامه ای، پرش، ویروس را فرا می خواند و ویروس اجرا می گردد، سپس ویروس قسمت ابتدائی فایل را به مکان اصلی اش باز می گرداند و اجازه اجرا شدن را به برنامه اصلی می دهد.

ویروسهای اسکریپتی فایل:

ویروسهای اسکریپتی واقعا شاخه مستقلی از ویروسها نیستند بلکه در حال حاضر جدی ترین تهدید به شمار می آیند.همانطور که قبلا توضیح داده شد اسکریپتها دستورات متنی خالصی هستند که باید توسط برخی برنامه ها تفسیر شوند.

زبانهای اسکریپتی تقریبا شامل انواع زیر می باشند:

- اسکریپت جاوا (Java Script)
- اسکریپت ویژوال بیسیک (VB Script)

- جی اسکریپت (JScript)

- اسکریپت شل یونیکس

- زبان بچ داس

- اسکریپت IRC

و ویژوال فاکس InstallShield- اسکریپتهای متفرقه مانند: سوپر لوگو، پرو و ...